UCRL-JC-123435 Abs

Remote Secure Proof of Identity by Biometrics

Sailes K. Sengupta, Lawrence Livermore National Laboratory, Livermore, CA 94550
Peter Pearson, Uptronics Incorporated, Sunnyvale, CA, 94088
and R. Scott Strait, Charles Schwab Inc., San Francisco, CA

We have demonstrated the remote secure proof of identity (POI) using biometrics. In this, maintaining the confidentiality of the individual's data is an important design consideration. The storage of any private biometrics data in a central database greatly increases the risk of compromise of the data. Equally important is to avoid transmission of the data over insecure communication channels. Cryptographic procedures are used in many applications to improve private data security. The risks of storage of the data can be greatly reduced if the data storage and POI are done using a smart card. However, this requires the individual to carry the smart card on their person

This research eliminates the need to store, anywhere, an individual's biometrics data while providing remote POI over public communications channels. Among other advantages, this technology (a) does not require an individual to carry a card, (b) does not require one to remember a password, (c) identifies an individual by statistically unique biometrics measurements, and (d) ensures that no private biometrics data is transmitted to, or stored in a database. This is accomplished by fully integrating an individual's biometrics into a public key cryptography algorithm after eliminating errors caused by statistical variations. We present here, how we incorporate a biometrics reading in a cryptographic protocol; the statistics of biometrics readings as bit strings of data; the use of error corrections to address the variability issue; and an implementation of the remote POI by biometrics using a specific biometrics device. It should be emphasized that the algorithm developed by us is largely independent of the biometrics device used.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.